Active Directory Integration

Session 608

These are confidential sessions—please refrain from filming or taking pictures.

Enterprise IT

Active Directory Integration

Joel Rennich
Consulting Engineer
Enterprise Consulting Group

http://developer.apple.com/wwdc2005/

Introduction

- What’s new in Tiger Client
- What’s new in Tiger Server
- AD Integration Scenarios
- Slaving AD to OD

What You'll Learn

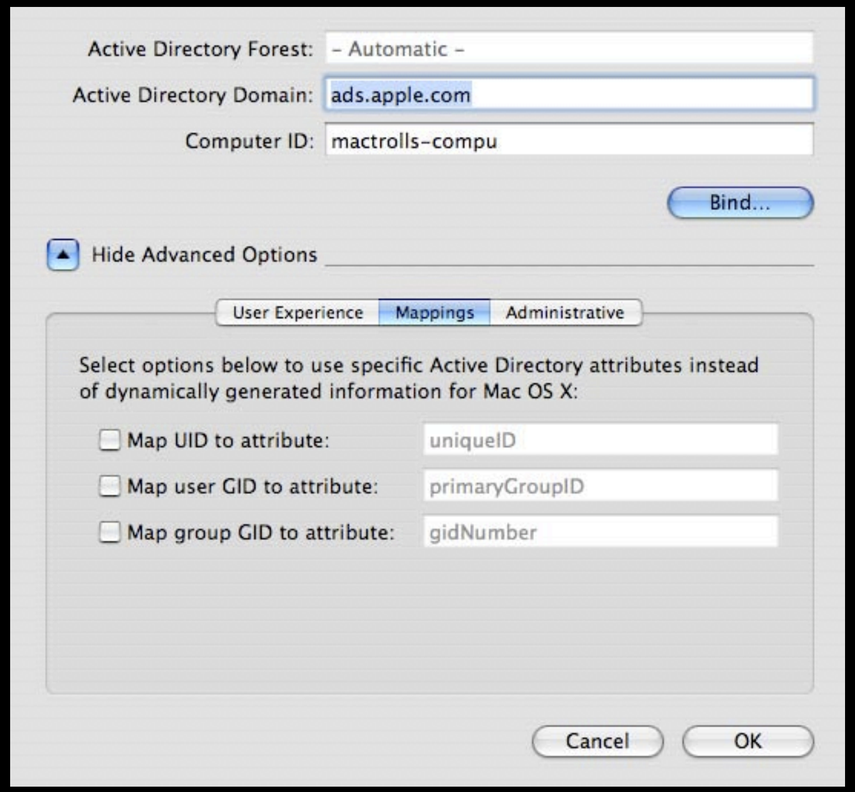
- How to integrate Tiger into Active Directory
  - Demos!
  - Troubleshooting the connection
- Ways to keep users in Active Directory but still have managed client settings for OS X
- How to keep passwords in Open Directory but still have Group Policies for Windows clients

What's New in Tiger Client

http://developer.apple.com/wwdc2005/

Group Membership

- Support for nested groups
- `memberd` now handles all group membership
  - No need for caching groups
  - Groups computed on the fly



Directory Access

- More options
- Most dsconfigad options in interface
- Automatically adds Active Directory domains to contacts and authentication tabs
- Map user primary group
- Map GID
- Check for dead domain controllers

dsconfigad

- Static mapping support
- Local admin user option so doesn’t have to run as root
- Should run much better in scripts

```
dsconfigad -f -a $COMPUTERNAME -forest
example.com -domain example.com -u administrator
-p 'password' -groups domain admins@example.com,
enterprise admins@example.com
```

Authentication

- NTLMv2 support
- Kerberos support for single sign on for home folder

Portable Home Directories

- Can work with AD users
  - Even if home is hosted on SMB
- Can login offline and synch when back on network
- Works mostly like you think it should

.local Domains

- Add .local domain to search domain in Network Preferences
  - Needs to be first
- Will resolve all .local addresses to regular DNS before going to mDNS

What We Don’t Do

- Signed SMB connections
- DFS

Connecting to Active Directory

AD Plugin Procedure

http://developer.apple.com/wwdc2005/

Binding to AD

1. Client requests _ldap._tcp., _kpasswd._tcp., _kerberos._tcp. SRV records from DNS
2. Client connects with LDAP to get basic AD domain information
3. AD plugin create edu.mit.Kerberos config file
4. Client authenticates and requests nearest Domain Controller
5. Receives back nearest DC
6. AD plugin recreates the edu.mit.Kerberos file with new DC
7. Client connects to the DC and searches domain for computer record
8. Create a new computer record if necessary

Files Involved

- /Library/Preferences/DirectoryService/ActiveDirectory.plist
  - Contains the plugin config and schema mappings
- /Library/Preferences/DirectoryService/SearchNodeConfig.plist
  - Contains the authentication path
- /Library/Preferences/DirectoryService/ContactsNodeConfig.plist
  - Contains the contacts path
- /Library/Preferences/edu.mit.Kerberos
  - Kerberos client configuration

Tiger Client Demo

Join Tiger Client to AD with script to automate process and evaluate AD joins

Eric Clements
Apple

http://developer.apple.com/wwdc2005/

AD Connections Troubleshooting

Getting more logging information

http://developer.apple.com/wwdc2005/

DirectoryService Debugging

- -USR1
  - killall -USR1 DirectoryService
  - On until -USR1 sent again
  - /Library//Logs/DirectoryService/DirectoryService.debug.log
- -USR2
  - killall -USR2 DirectoryService
  - API level debugging
  - Only on for 5 mins
  - Same log

Starting Over

- Delete appropriate preferences file in /Library/Preferences/DirectoryServices
  - ActiveDirectory.plist
  - SearchNodeConfig.plist
  - ContactsNodeConfig.plist
- Restart DirectoryService
  - killall DirectoryService
- Restart lookupd
  - killall lookupd
- Relaunch Directory Access

Demo

Troubleshooting AD

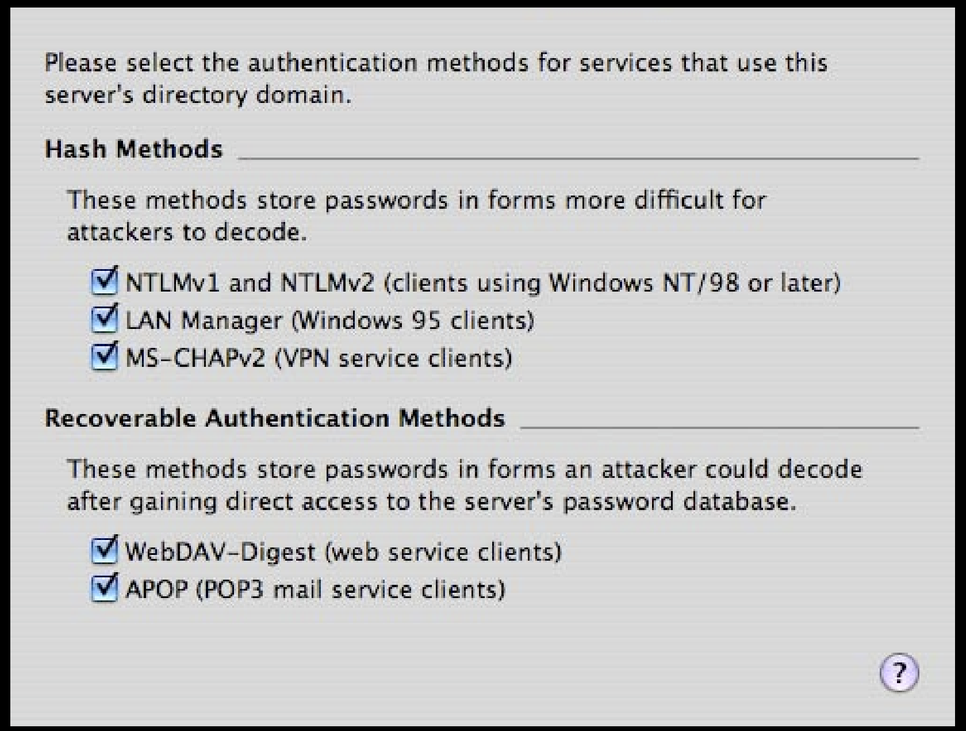
Eric Clements
Apple

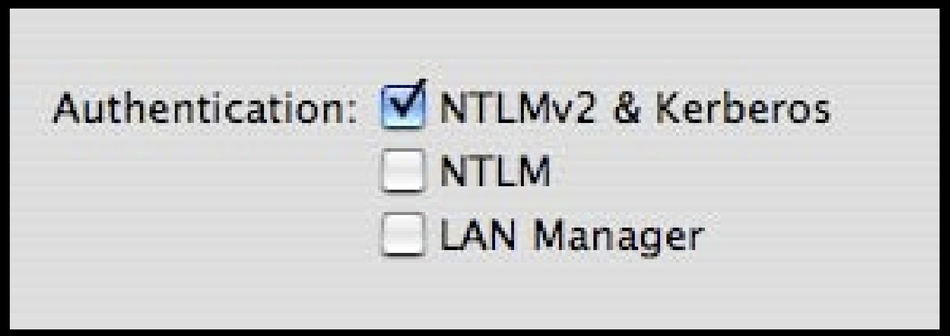
http://developer.apple.com/wwdc2005/

Tiger Server

Changes in 10.4 Server

http://developer.apple.com/wwdc2005/



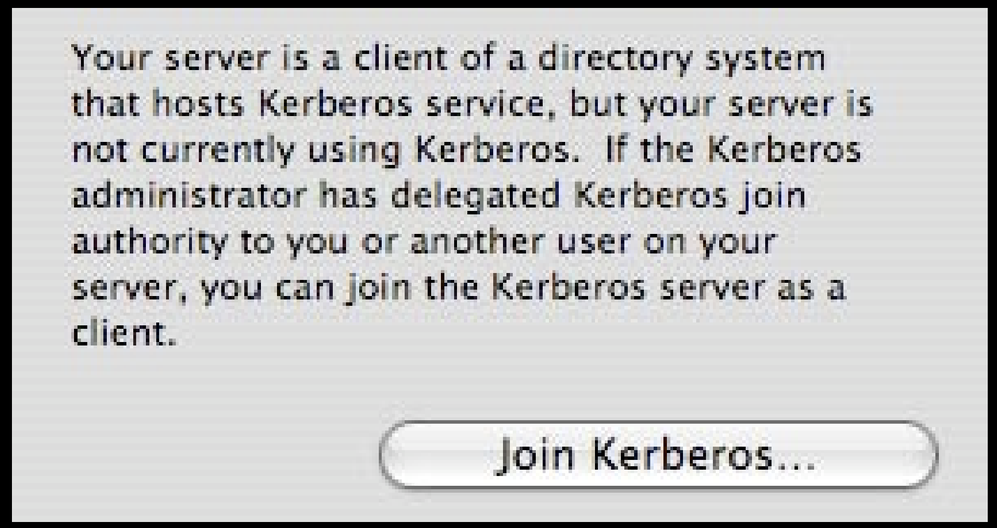


Authentication

- NTLMv2 support for SMB shares
  - Checkbox in Server Admin for SMB password types
- Actual Kerberos keytab for SMB
- Can disable LanManager and NTLM hashes from PasswordServer from Server Admin
  - No need for NeST command

Access Control Lists

- ACL enabled file systems will allow Windows users to control ACLs with Windows tools
- Same ACLs as Windows



Kerberos

- Join Kerberos Realm
  - Single click in Server Admin
  - Also dsconfigad -enableSSO
  - Creates keytab entries for AFP, SMB, FTP, Host, IMAP, POP, SMTP and others
  - No need to touch Domain Controller

All other client changes

- dsconfigad
- memberd for group resolution
- Discovers dead Active Directory controllers when joining

Tiger Server Demo

One-click Kerberos integration

Eric Clements
Apple

http://developer.apple.com/wwdc2005/

Deployment Options

Using Active Directory for users, but still managing with MCX

http://developer.apple.com/wwdc2005/

Extend the Schema

- Single point of control
- Somewhat invasive to Active Director, especially Windows 2000
- User and group controls, and machines with some extra work
- Use Workgroup Manager for all MCX needs

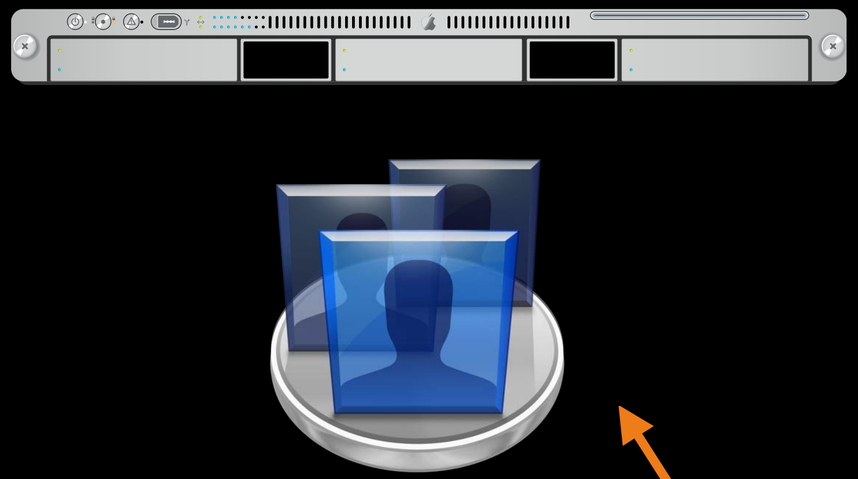
Instructions
http://images.apple.com/server/pdfs/Open_Directory_v10.4.pdf

AD Plugin

Magic Triangle

- Keep MCX in Open Directory
- Join clients to Active Directory and Open Directory
- Manage MCX by group or machine in Open Directory

Instructions
http://www.afp548.com/



LDAP

AD Plugin

Kerberos Cross Realm

Open Directory as top dog

http://developer.apple.com/wwdc2005/

Reverse Magic Triangle

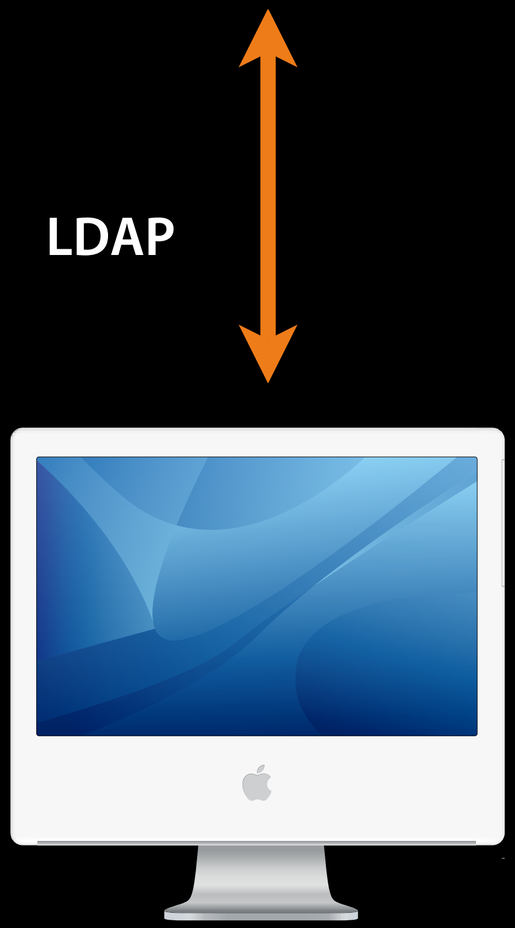
- Active Directory uses Open Directory for passwords
- Still allows AD for Windows Client management but maintain central password store
- Don’t need to synch passwords, but do need to synch user records

Instructions
http://www.4am-media.com/xrealm/

Passwords

X-Realm

LDAP



Active Directory

More Information

http://developer.apple.com/wwdc2005/

Documentation, Sample Code, and Other Resources

http://developer.apple.com/wwdc2005/

Q&A

http://developer.apple.com/wwdc2005/

WWDC2005

Worldwide Developers Conference